FUDO SECURITY

ZERO TRUST NETWORK ACCESS:

what is it, and why does it matter?

Zero Trust is not a new security architecture. Its origins date back to the 90s. However, it has recently been gaining popularity once again.

The central assumption of Zero Trust Network Access is that users in the system begin their access journey with the lowest possible level of authorization and ensure that everything is verified at every step.

This article will show that this type of approach gives us the best chance of winning the fight against attacks on organizations.

Insider Threat, or is it a threat coming „from the inside".

According to an analysis by Cybersecurity Insiders Insiders[1] in 2020, **68% of organizations are most afraid of threats posed by their employees.** It's hardly surprising. Let's take a look at a few high-profile attacks on Amazon or Twitter, where the internal staff turned out to be the main threat to the company.

[1] https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf

If we have a closer look at the Twitter example, it turns out that the problem was not a simple desire to harm the company.

From year-to-year, social engineering attacks have become ever more complicated, and sometimes, even security professionals find it challenging to recognize this type of attack. This was the case with Twitter, as employees lost their credentials, giving attackers access to the firm's internal administration tools. **This led to another social engineering attack - this time directly targeting Twitter users.**

Another high-profile incident involved Tesla - The attacker offered an employee over a million dollars to install ransomware.
Fortunately, this time the attack was unsuccessful.

The awareness of threats in the network is constantly growing, and companies pay more and more attention to network and information security.

So why are there still so many high-profile hacking attacks?
The question is whether humans are the weakest link in the security of the system.

The idea of limited trust in employees – a bull's-eye or an own goal?

As recent attacks have shown, it is better to restrict users' rights.
It must be remembered that the more power and access someone has, the more attractive a target they become for attackers.

There is also much greater responsibility associated with elevated powers and access. Even if employees don't intend to harm the organization, they can simply make a mistake that, like snowballing, will cause enormous losses and damage for the company.

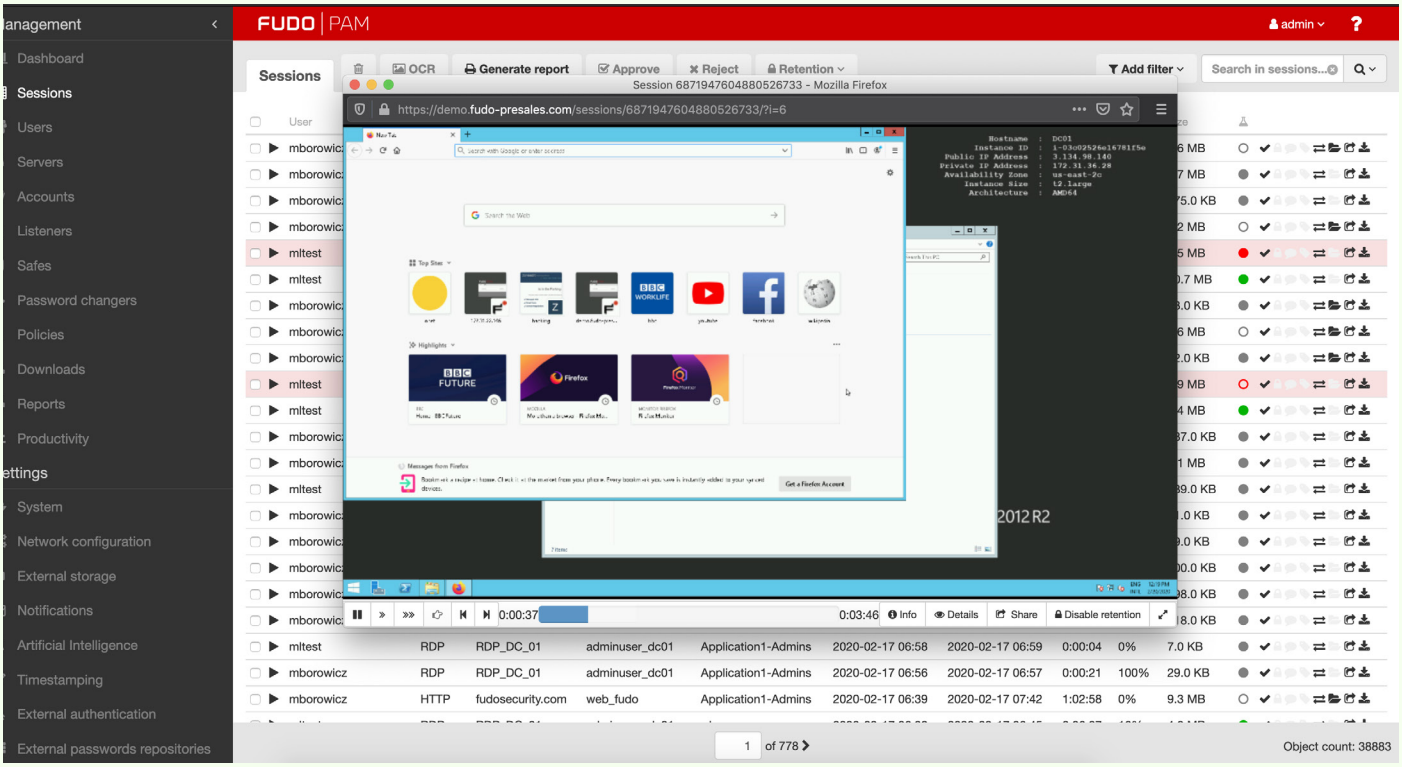
How do you implement Zero Trust Network Access in a company?

This architecture is not associated with any specific technology. It can be used in both network administration and software development. We then assume that our system components should have limited access.

Suppose we would like to apply Zero Trust architecture in our organization. In that case, we should assume that everything outside the company, and above all within the organization itself, is potentially vulnerable.

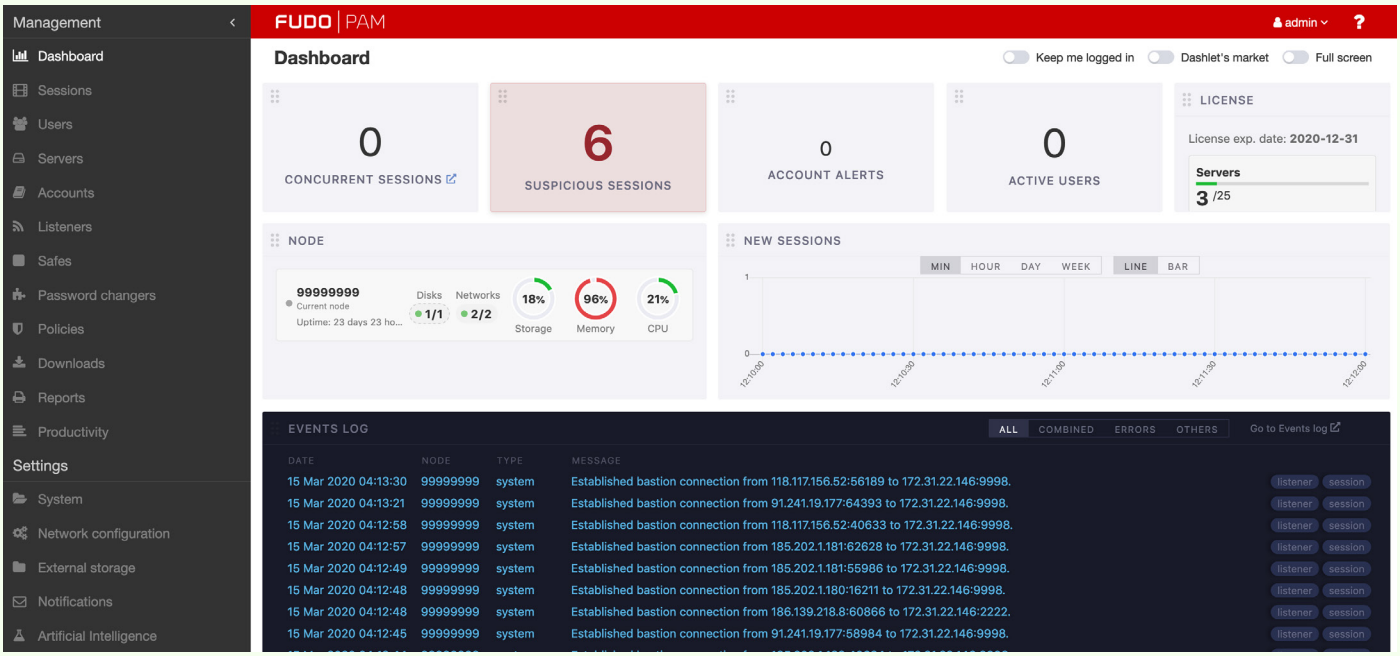
Therefore, we should avoid a user with broad access and **verify each individual access to network resources.** It would even be recommended to go one step further. How? Not only to verify access to individual systems but also to individual actions performed on these systems.

Zero Trust Network Access also assumes continuous verification. This means that **all user actions should be recorded and analyzed** - this will enable faster detection of attacks and mitigate their effects.



Our security model can also apply the 4-eye authentication method where one administrator confirms the other's access to critical company resources or approves unknown or dangerous commands

performed on servers. If such technology had been used at Twitter, perhaps the administration tool would ask for the suspicious actions to be confirmed by another administrator who could have quickly reacted, and the attack would have been avoided.



Zero Trust architecture seems to be the future of the IT security industry. It will provide organizations with transparent employee activities, accountability and even save them from costly errors.

Mariusz Zaborski

Mariusz is DEV & QA manager at Fudo Security. His main interests are the security of operating systems and low-level programming.

Mariusz is an active committer of the FreeBSD community, and in his spare time, he runs a blog.